Werk

Titel: Discriminants of certain algebraic number fields.

Autor: Komatsu, Kenzo

Jahr: 1976

PURL: https://resolver.sub.uni-goettingen.de/purl?243919689_0285|log16

Discriminants of certain algebraic number fields

By *Kenzô Komatsu* at Tôkyô

The main purpose of this paper is to prove Theorem 1, Theorem 2 and Theorem 3 in § 3. Let A, B and $n (n > 1)$ be rational integers such that

$$f(x) = x^n + Ax + B$$

is irreducible over the rational number field. In our previous paper [2], we studied the algebraic number field K of degree n defined by $f(x) = 0$. Assuming certain conditions on A, B and n, we obtained an integral basis and the discriminant of K. In the present paper, we study the discriminant of the minimal splitting field of $f(x) = 0$. One of the simplest cases will be treated in Theorem 1. More complicated cases will be discussed in Theorem 2 and Theorem 3. To prove these theorems we require some results of our previous paper [2]. We also require some lemmas on ramification theory, which will be described in § 2. In particular, Lemma 1 plays a fundamental rôle throughout this paper. As another application of this lemma, certain properties of algebraic number fields of prime degree will be discussed in § 4. For a general discussion of ramification theory, the reader is referred to Hilbert [1].

A special case of our Theorem 1 was treated in Uchida [5], [6] and Yamamoto [7] in connexion with unramified extensions of quadratic number fields. The author is grateful to Dr. N. Adachi for his advice and criticism.

1. Notation and terminology

For a prime number p and a rational integer a, a_p denotes the largest integer m such that a is divisible by p^m, i.e.

$$p^{a_p} \mid a,\ p^{a_p+1} \nmid a.$$

When $a = 0$, we define $a_p = \infty$. We denote the ring of rational integers by $\mathbb{Z}$, the rational number field by $\mathbb{Q}$, the order of a finite group G by $|G|$, and the norm (resp. the relative norm with respect to K/k) of an ideal $\mathfrak{a}$ by $N(\mathfrak{a})$ (resp. $N_{K/k}(\mathfrak{a})$). The notation $[X : Y]$ means either the index of a subgroup Y of a group X, or the degree of a finite extension X of a field Y.

An algebraic number field always means an algebraic number field of *finite degree*. Let K, k be algebraic number fields such that $K \supset k$. Then the minimal algebraic number field $\bar{K}$ such that (i) $\bar{K}/k$ is normal, (ii) K is contained in $\bar{K}$ (in other words, the composition of all the conjugate fields of K over k), is called *the Galois closure of* K/k. If $\bar{\mathfrak{P}}$ is a prime ideal in $\bar{K}$, *the i-th ramification group* V_i *of* $\bar{\mathfrak{P}}$ *with respect to* $\bar{K}/k$ is defined by

$$V_i = \{v \in Z,\ \alpha^v \equiv \alpha (\mathrm{mod}\ \bar{\mathfrak{P}}^{i+1}) \text{ for every integer } \alpha \text{ of } \bar{K}\},$$

where Z is the decomposition group of $\bar{\mathfrak{P}}$ with respect to $\bar{K}/k$, $i \geqq 0$. If M is a subset of a group G, the group

$$\{g \in G,\ gm = mg \quad \text{for every} \quad m \in M\}$$

is called *the centralizer of* M *in* G.

2. General preliminaries

Lemma 1. *Let K, k be algebraic number fields such that $K \supset k$ and let $\bar{K}$ be the Galois closure of K/k. Let $\mathfrak{p}$ be a prime ideal in k and let $\mathfrak{P}_1, \ldots, \mathfrak{P}_s$ be distinct prime ideals in K such that*

$$\mathfrak{p} = \mathfrak{P}_1^{e_1} \ldots \mathfrak{P}_s^{e_s},\ N_{K/k}(\mathfrak{P}_i) = \mathfrak{p}^{f_i}.$$

Further let

p:	*the prime number divisible by* $\mathfrak{p}$,
$\bar{\mathfrak{P}}$:	*a prime ideal in* $\bar{K}$ *which divides* $\mathfrak{p}$,
G:	*the Galois group of* $\bar{K}/k$,
H:	*the Galois group of* $\bar{K}/K$,
Z:	*the decomposition group of* $\bar{\mathfrak{P}}$ *with respect to* $\bar{K}/k$,
T:	*the inertia group of* $\bar{\mathfrak{P}}$ *w. r. to* $\bar{K}/k$,
V:	*the first ramification group of* $\bar{\mathfrak{P}}$ *w. r. to* $\bar{K}/k$,
$C(T)$:	*the centralizer of* T *in* Z,
$C(V)$:	*the centralizer of* V *in* T,
$Aut(T)$:	*the group of automorphisms of* T,
$Aut(V)$:	*the group of automorphisms of* V,
$E = \lvert T \rvert$:	*the ramification index of* $\mathfrak{p}$ *w. r. to* $\bar{K}/k$,
$F = \lvert Z/T \rvert$:	*the relative degree of* $\mathfrak{p}$ *w. r. to* $\bar{K}/k$,
a:	*the least common multiple of* $e_1, \ldots, e_s$,
b:	*the least common multiple of* $f_1, \ldots, f_s$,
a':	*the least common multiple of the* $\dfrac{e_i}{p^{(e_i)_p}}$, $1 \leqq i \leqq s$.

Then:

(a) *$C(V)$ is a normal subgroup of T, and $T/C(V)$ is isomorphic to a subgroup of $Aut(V)$.*
(b) *$C(T)$ is a normal subgroup of Z, and $Z/C(T)$ is isomorphic to a subgroup of $Aut(T)$.*
(c) *If $t \in C(V)$, $t^{a'} \in V$.*
(d) *$[T: V] = a'm'$, where m' is an integer which divides $\lvert Aut(V) \rvert$.*
(e) *If $z \in C(T)$, $z^{bE} = 1$.*
(f) *$F = bm$, where m is an integer which divides $E \lvert Aut(T) \rvert$.*
(g) *If $p \nmid a$, then $E = a$, $F = bm$, $m \mid a\varphi(a)$, where $\varphi(a)$ is the number of rational integers x such that $0 < x \leqq a$, $(x, a) = 1$.*
(h) *If $\mathfrak{p}$ is unramified in K/k, $F = b$.*
(i) *If $p > \dfrac{[K:k]}{2}$, $p - 1$ is divisible by the integer $\dfrac{E}{a}$.*

Proof. For every $t \in T$, $v \to t^{-1}vt$ is an automorphism of V, since V is normal in T. This defines a homomorphism of T into $Aut(V)$ with kernel $C(V)$. Thus we obtain (a). Similarly, since T is normal in Z, we obtain (b).

For any $g \in G$, $(T \cap gHg^{-1})/(V \cap gHg^{-1})$ is contained (canonically) in the cyclic group T/V. If $\mathfrak{P}^g \mid \mathfrak{P}_i$,

$$[T/V : (T \cap gHg^{-1})/(V \cap gHg^{-1})] = \frac{[T : T \cap gHg^{-1}]}{[V : V \cap gHg^{-1}]} = \frac{[g^{-1}Tg : g^{-1}Tg \cap H]}{[g^{-1}Vg : g^{-1}Vg \cap H]} = \frac{e_i}{p^{(e_i)_p}}.$$

Hence, if $t \in T$, $t^{a'} = t_0 v$, where $t_0 \in T \cap gHg^{-1}$, $v \in V$. Now suppose that $t \in C(V)$. Then, since $v^P = 1$, where $P = p^{E_p}$, we have

$$t^{a'P} = (t^{a'}v^{-1})^P = t_0^P \in gHg^{-1}.$$

Now $\bar{K}$ is the Galois closure of K/k, so that

$$\bigcap_{g \in G} gHg^{-1} = \{1\}.$$

Hence $t^{a'P} = 1$. Since $[T : V]$ is prime to p, we obtain (c). Since $[T : V]$ is divisible by $\frac{e_i}{p^{(e_i)_p}}$ for every i, $[T : V]$ is divisible by a', i.e.

$$[T : V] = a'm', \quad m' \in \mathbb{Z}.$$

Let $t_1 V$ ($t_1 \in T$) be a generator of the cyclic group T/V. Then it follows from (a) and (c) that

$$t_1^{|Aut(V)|a'} \in V,$$

which proves (d).

For any $g \in G$, $(Z \cap gHg^{-1})/(T \cap gHg^{-1})$ is contained (canonically) in the cyclic group Z/T, and

$$[Z/T : (Z \cap gHg^{-1})/(T \cap gHg^{-1})] = \frac{[Z : Z \cap gHg^{-1}]}{[T : T \cap gHg^{-1}]} = f_i$$

for a certain i. If $z \in C(T)$, $z^b = z_0 t$, where $z_0 \in Z \cap gHg^{-1}$, $t \in T$. Hence

$$z^{bE} = (z^b t^{-1})^E \in gHg^{-1},$$

which proves (e). Since F is divisible by f_i for every i, F is divisible by b, i.e.

$$F = bm, \quad m \in \mathbb{Z}.$$

Let $z_1 T$ ($z_1 \in Z$) be a generator of the cyclic group Z/T. Then it follows from (b) and (e) that

$$z_1^{|Aut(T)|bE} = 1,$$

which proves (f).

For each $g \in G$, we have

$$[V : V \cap gHg^{-1}] = [g^{-1}Vg : g^{-1}Vg \cap H] = p^{(e_i)_p}$$

for a certain i. If $p \nmid a$, $[V : V \cap gHg^{-1}] = 1$, i.e. V is contained in gHg^{-1} for every $g \in G$.

This implies $V=\{1\}$. From (d) and (f), we obtain (g) and (h).

The assertion (i) is obvious if $p \nmid a$. If $p|a$, then $E_p=1$, since $[\bar{K}:k]|[K:k]!$. Hence V is a cyclic group of order p and so $|Aut(V)|=p-1$. Since $e_i=p$ for a certain i, we have $a=pa'$. Now the result follows immediately from (d). This completes the proof.

Lemma 2. *Let K be an algebraic number field, $\bar{K}$ the Galois closure of $K/\mathbb{Q}$, $\bar{d}$ the discriminant of $\bar{K}$, and $N=[\bar{K}:\mathbb{Q}]$. Let p be a prime number and let $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ be distinct prime ideals in K such that*

$$p=\mathfrak{p}_1^{e_1}\ldots\mathfrak{p}_s^{e_s}.$$

If $p \nmid e_i$ for every i, then

$$\bar{d}_p=N\left(1-\frac{1}{a}\right),$$

where a is the least common multiple of $e_1, \ldots, e_s$.

Proof. It follows from Lemma 1, (g) that the ramification index E of p with respect to $\bar{K}/\mathbb{Q}$ is equal to a. Hence we obtain

$$\bar{d}_p=\frac{N}{E}(E-1)=N\left(1-\frac{1}{a}\right),$$

since E is not divisible by p (see Hilbert [1], Satz 79).

Lemma 3. *Let K be an algebraic number field of degree n, p a prime number with $p>\frac{n}{2}$, and $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ distinct prime ideals in K such that*

$$p=\mathfrak{p}_1^{e_1}\ldots\mathfrak{p}_s^{e_s},\ N(\mathfrak{p}_i)=p^{f_i}.$$

Further let

$\bar{K}$:	*the Galois closure of $K/\mathbb{Q}$, $N=[\bar{K}:\mathbb{Q}]$,*
d:	*the discriminant of K,*
$\bar{d}$:	*the discriminant of $\bar{K}$,*
E:	*the ramification index of p with respect to $\bar{K}/\mathbb{Q}$,*
$\bar{\mathfrak{p}}$:	*a prime ideal in $\bar{K}$ which divides p,*
V_i $(i\geqq 0)$:	*the i-th ramification group of $\bar{\mathfrak{p}}$ with respect to $\bar{K}/\mathbb{Q}$,*
u:	*the minimum integer i such that $i\geqq 0$, $V_{i+1}=\{1\}$,*
a:	*the least common multiple of $e_1, \ldots, e_s$.*

Then

$$d_p=n-\sum_{i=1}^{s} f_i+\frac{p(p-1)u}{E},$$

$$\bar{d}_p=\begin{cases} N\left(1-\frac{1}{E}\right)=N\left(1-\frac{1}{a}\right) & (p \nmid a) \\ \frac{N}{E}\{E-1+(p-1)u\} & (p|a). \end{cases}$$

Proof. Suppose that $p \nmid a$. Then $u=0$ (Lemma 1, (g)). On the other hand (Hilbert [1], §12)

$$d_p = \sum_{i=1}^{s} (e_i - 1) f_i = n - \sum_{i=1}^{s} f_i.$$

Next suppose that $p \mid a$. Since $p > \frac{n}{2}$, and u is independent of the choice of $\bar{\mathfrak{p}}$, we may suppose that $e_1 = p$, $\bar{\mathfrak{p}} \mid \mathfrak{p}_1$. Let $\mathfrak{d}$ be the different of $K/\mathbb{Q}$. For every i, suppose that $\mathfrak{d}$ is divisible exactly by $\mathfrak{p}_i^{D(i)}$. Since $N \mid n!$, we have $E_p = 1$ and so $V_1 \cap H = \{1\}$, where H is the Galois group of $\bar{K}/K$. Hence

$$D(1) = (e_1 - 1) + \frac{p(p-1)u}{E},$$

and $D(i) = e_i - 1$ for every $i > 1$ (Hilbert [1], Satz 41, Satz 79 and §12). Since $f_1 = 1$, it follows that

$$d_p = \sum_{i=1}^{s} D(i) f_i = \sum_{i=1}^{s} (e_i - 1) f_i + \frac{p(p-1)u}{E}.$$

The last equality follows immediately from Hilbert [1], Satz 79.

Lemma 4. *Let $a(0), a(1), \ldots, a(n-1)$ be rational integers $(n \geqq 1)$ and let p be a prime number such that*

$$0 < a(0)_p \leqq a(i)_p \quad (0 \leqq i \leqq n-1),\ (a(0)_p, n) = 1.$$

Then

$$f(x) = x^n + \sum_{i=0}^{n-1} a(i)\, x^i$$

is irreducible over $\mathbb{Q}$, and $p = \mathfrak{p}^n$, $\mathfrak{p}$ a prime ideal, in $\mathbb{Q}(\alpha)$, where α is an arbitrary root of $f(x) = 0$.

Proof. Let α be an arbitrary root of $f(x) = 0$, and $\mathfrak{p}$ a prime ideal in $\mathbb{Q}(\alpha)$ which divides p. Suppose that α (resp. p) is divisible exactly by $\mathfrak{p}^m$ (resp. $\mathfrak{p}^e$) in $\mathbb{Q}(\alpha)$. By hypothesis, $m > 0$. Since

$$-\alpha^n = \sum_{i=0}^{n-1} a(i)\, \alpha^i,$$

we have $nm = e a(0)_p$. Since $(a(0)_p, n) = 1$, it follows that

$$n \leqq e \leqq [\mathbb{Q}(\alpha) : \mathbb{Q}] \leqq n.$$

This completes the proof.

3. Main results

Theorem 1. *Let n $(n > 1)$, A, B be rational integers such that $f(x) = x^n + Ax + B$ is irreducible over $\mathbb{Q}$, $\alpha^{(1)}, \ldots, \alpha^{(n)}$ the roots of $f(x) = 0$, and $\bar{d}$ the discriminant of*

$$\bar{K} = \mathbb{Q}(\alpha^{(1)}, \ldots, \alpha^{(n)}).$$

Let p be a prime number which satisfies none of the following conditions:

(1) $p|n,\quad 0<B_p\leqq A_p,$

(2) $p|n-1,\quad 0<A_p<B_p,$

(3) $p|n,\quad A_p>0,\quad B_p=0,$

(4) $p|n-1,\quad A_p=0,\quad B_p>0,$

(5) $A_p\geqq n-1,\quad B_p\geqq n.$

Let E be the ramification index of p with respect to $\bar{K}/\mathbb{Q}$, and let $N=[\bar{K}:\mathbb{Q}]$,

$$D=(-1)^{n-1}(n-1)^{n-1}A^n+n^n B^{n-1}.$$

Then

$$\bar{d}_p=N\left(1-\frac{1}{E}\right).$$

Moreover, the value of E is given by the following table.

p	E
$p\|D,\ A_p=B_p=0,\ D_p$ odd	2
$0<A_p<B_p$	$\dfrac{n-1}{(n-1,\ A_p)}$
$0<B_p\leqq A_p$	$\dfrac{n}{(n,\ B_p)}$
Otherwise	1

Remark. The condition (5) is not essential. Let r be the largest positive integer such that $r^{n-1}|A$, $r^n|B$. Put

$$A'=\frac{A}{r^{n-1}},\quad B'=\frac{B}{r^n},\quad \alpha'=\frac{\alpha^{(1)}}{r}.$$

Then α' is a root of

$$x^n+A'x+B'=0,$$

and there is no prime number q which satisfies $A'_q\geqq n-1$, $B'_q\geqq n$. Moreover

$$D'=(-1)^{n-1}(n-1)^{n-1}A'^n+n^n B'^{n-1}=\frac{D}{r^{n(n-1)}}.$$

If a prime number p does not satisfy the condition (5), then $A_p=A'_p$, $B_p=B'_p$ and $D_p=D'_p$. Therefore we can use Theorem 3 of our previous paper [2].

Proof. Suppose that $p|\bar{d}$. Then $A_p=B_p=0$ or $A_p>0$, $B_p>0$, since $p|D$. The result follows from Lemma 1, (g), Lemma 2 and Komatsu [2], Theorem 2, the proof of Theorem 3.

Theorem 2. *Let p be a prime number and let A, B be rational integers such that $f(x)=x^p+Ax+B$ is irreducible over $\mathbb{Q}$. Let*

$\alpha^{(1)}, \ldots, \alpha^{(p)}$: *the roots of* $f(x)=0$,
d: *the discriminant of* $K=\mathbb{Q}(\alpha^{(1)})$,
$\bar{d}$: *the discriminant of* $\bar{K}=\mathbb{Q}(\alpha^{(1)}, \ldots, \alpha^{(p)})$,
E: *the ramification index of* p *with respect to* $\bar{K}/\mathbb{Q}$,
$\bar{\mathfrak{p}}$: *a prime ideal in* $\bar{K}$ *which divides* p,
V_i $(i \geqq 0)$: *the* i*-th ramification group of* $\bar{\mathfrak{p}}$ *with respect to* $\bar{K}/\mathbb{Q}$,
u: *the minimum integer* i *such that* $i \geqq 0$, $V_{i+1}=\{1\}$; $N=[\bar{K}:\mathbb{Q}]$.

Suppose that p satisfies none of the following conditions:

(1) $A_p=1, \quad B_p=0$,
(2) $A_p=B_p>0, \quad (B_p, p-1)\neq 1$,
(3) $A_p \geqq p-1, \quad B_p \geqq p$.

Then the values of d_p, E, u and $\bar{d}_p$ are given by the following table.

p	d_p	E	u	$\bar{d}_p$
$A_p>B_p>0$	$2p-1$	$p(p-1)$	p	$\dfrac{N(2p^2-2p-1)}{p(p-1)}$
$A_p=B_p>0$	B_p+p-1	$p(p-1)$	B_p	$\dfrac{N}{p}\left(B_p+p-\dfrac{1}{p-1}\right)$
$0<A_p<B_p$	$p-1-(p-1, A_p)$	$\dfrac{p-1}{(p-1, A_p)}$	0	$\dfrac{N(p-1-(p-1, A_p))}{p-1}$
$A_p>0, B_p=0,$ $(-B)^{p-1}\not\equiv 1 \pmod{p^2}$	p	$p(p-1)$	1	$\dfrac{N(p^2-2)}{p(p-1)}$
$A_p>0, B_p=0,$ $(-B)^{p-1}\equiv 1 \pmod{p^2}$	$p-2$	$p-1$	0	$\dfrac{N(p-2)}{p-1}$
Otherwise	0	1	0	0

Proof. (See the remark of Theorem 1.) Suppose that $A_p>B_p>0$. Since $(p, B_p)=1$, it follows from [2], Theorem 3, (2) that

$$d_p=D_p-(p-1)(B_p-1)=2p-1,$$

where $D=(-1)^{p-1}(p-1)^{p-1}A^p+p^pB^{p-1}$. On the other hand, from Lemma 3 and Lemma 4, we obtain

$$(*) \qquad d_p=p-1+\frac{p(p-1)u}{E}.$$

Hence

$$\frac{p(p-1)u}{E}=p.$$

Now $p-1$ is divisible by $\frac{E}{p}$ (Lemma 1, (i)). Hence

$$\frac{E}{p}=p-1, \quad u=p.$$

From Lemma 3 we obtain

$$\bar{d}_p=\frac{N(2p^2-2p-1)}{p(p-1)}.$$

Next, suppose that $A_p=B_p>0$. Since $D_p=pB_p$, it follows from [2], Theorem 3, (2) that

$$d_p=pB_p-(p-1)(B_p-1)=B_p+p-1.$$

From (*) we obtain

$$B_p=\frac{p(p-1)u}{E}.$$

Now $(B_p, p-1)=1$ by hypothesis, and $p-1$ is divisible by $\frac{E}{p}$ (Lemma 1, (i)). Hence

$$\frac{E}{p}=p-1, u=B_p, \bar{d}_p=\frac{N}{p}\left(B_p+p-\frac{1}{p-1}\right).$$

Now suppose that $A_p>0$, $B_p=0$. By hypothesis, $A_p>1$. If $(-B)^{p-1}\not\equiv 1 \pmod{p^2}$, then $p=\mathfrak{p}^p$ in K, $d_p=D_p=p$ ([2], Theorem 5 and its proof). From (*), Lemma 1, (i) and Lemma 3, we obtain

$$\frac{E}{p}=p-1, u=1, \bar{d}_p=\frac{N(p^2-2)}{p(p-1)}.$$

Now suppose that $(-B)^{p-1}\equiv 1 \pmod{p^2}$. Let $\alpha=\alpha^{(1)}$ and let $\mathfrak{a}$ denote the ideal in K generated by p and $-B-\alpha$:

$$\mathfrak{a}=(p, -B-\alpha).$$

Then $\mathfrak{a}$ is divisible by every prime factor of p, $d_p=p-2$, $N(\mathfrak{a})=p^2$ and $p=\prod \mathfrak{p}_i^{e_i}$, $N(\mathfrak{p}_i)=p^{f_i}$, $\sum f_i=2$ ([2], Theorem 5 and its proof). If $p=2$, then $d_p=0$, $E=1$, $u=0$, $\bar{d}_p=0$. If $p\neq 2$, $\mathfrak{a}$ cannot be a prime ideal or the square of a prime ideal. Hence $\mathfrak{a}=\mathfrak{p}_1\mathfrak{p}_2$, $\mathfrak{p}_1\neq\mathfrak{p}_2$, $p=\mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}$, $e_1>e_2$. Since $\mathfrak{a}^{e_1}$ is divisible by p, $\frac{(-B-\alpha)^{e_1}}{p}$ is an integer of K. Hence $e_1\geqq p-1$ ([2], Theorem 5, (2). Note that $r_p=1$). Now the result follows from Lemma 1, (g), Lemma 2, Theorem 1 and [2], Theorem 3, (4).

Theorem 3. *Let p be a prime number and let A, B be rational integers such that $f(x)=x^{p+1}+Ax+B$ is irreducible over $\mathbb{Q}$. Let*

$\alpha^{(1)}, \ldots, \alpha^{(p+1)}$:	*the roots of $f(x)=0$,*
d:	*the discriminant of $K=\mathbb{Q}(\alpha^{(1)})$,*
$\bar{d}$:	*the discriminant of $\bar{K}=\mathbb{Q}(\alpha^{(1)}, \ldots, \alpha^{(p+1)})$,*
E:	*the ramification index of p with respect to $\bar{K}/\mathbb{Q}$,*
$\bar{\mathfrak{p}}$:	*a prime ideal in $\bar{K}$ which divides p,*
V_i $(i\geqq 0)$:	*the i-th ramification group of $\bar{\mathfrak{p}}$ with respect to $\bar{K}/\mathbb{Q}$,*
u:	*the minimum integer i such that $i\geqq 0$, $V_{i+1}=\{1\}$; $N=[\bar{K}:\mathbb{Q}]$.*

Suppose that p satisfies none of the following conditions:

(1) $A_p=0, \quad B_p=1,$

(2) $0<A_p=B_p-1, \quad (p-A_p, p-1)\neq 1,$

(3) $A_p\geqq p, \quad B_p\geqq p+1.$

Then the values of d_p, E, u *and* $\bar{d}_p$ *are given by the following table.*

p	d_p	E	u	$\bar{d}_p$
$A_p\geqq B_p>0$	$p+1-(p+1, B_p)$	$\dfrac{p+1}{(p+1, B_p)}$	0	$\dfrac{N(p+1-(p+1, B_p))}{p+1}$
$0<A_p<B_p-1$	$2p-1$	$p(p-1)$	p	$\dfrac{N(2p^2-2p-1)}{p(p-1)}$
$0<A_p=B_p-1$	$2p-1-A_p$	$p(p-1)$	$p-A_p$	$\dfrac{N}{p}\left(2p-A_p-\dfrac{1}{p-1}\right)$
$A_p=0, B_p>0,$ $(-A)^{p-1}\not\equiv 1 \pmod{p^2}$	p	$p(p-1)$	1	$\dfrac{N(p^2-2)}{p(p-1)}$
$A_p=0, B_p>0,$ $(-A)^{p-1}\equiv 1 \pmod{p^2}$	$p-2$	$p-1$	0	$\dfrac{N(p-2)}{p-1}$
Otherwise	0	1	0	0

Proof. (See the remark of Theorem 1.) Suppose that $0<A_p<B_p-1$. Then

$$d_p=D_p-(p+1)A_p+(p-1)=2p-1,$$

where $D=(-1)^p p^p A^{p+1}+(p+1)^{p+1}B^p$ ([2], Theorem 3, (5)). Since $p=\mathfrak{q}\mathfrak{p}^p$ $(\mathfrak{p}\neq\mathfrak{q})$ in K ([2], the proof of Theorem 3), it follows from Lemma 3 that

$$(*) \qquad d_p=(p-1)+\frac{p(p-1)u}{E}.$$

Now $p-1$ is divisible by $\dfrac{E}{p}$ (Lemma 1, (i)). Hence

$$\frac{E}{p}=p-1, \ u=p, \ \bar{d}_p=\frac{N(2p^2-2p-1)}{p(p-1)}.$$

Next, suppose that $0<A_p=B_p-1$. Since $D_p=pB_p$, it follows from [2], Theorem 3, (5) that

$$d_p=pB_p-(p+1)A_p+(p-1)=p-A_p+(p-1).$$

From (*) we obtain

$$p-A_p=\frac{p(p-1)u}{E}.$$

By hypothesis, $(p-A_p, p-1)=1$. Since $p-1$ is divisible by $\frac{E}{p}$ (Lemma 1, (i)), it follows that

$$\frac{E}{p}=p-1,\ u=p-A_p,\ \bar{d}_p=\frac{N}{p}\left(2p-A_p-\frac{1}{p-1}\right).$$

Now suppose that $A_p=0$, $B_p>0$. By hypothesis, $B_p>1$. Let $\alpha=\alpha^{(1)}$ and let $\mathfrak{q}$ denote the prime ideal in K generated by p and $-\alpha$:

$$\mathfrak{q}=(p,\ -\alpha).$$

If $(-A)^{p-1}\not\equiv 1 \pmod{p^2}$, then $p=\mathfrak{q}\mathfrak{p}^p$ $(\mathfrak{p}\neq\mathfrak{q})$ in K, $d_p=D_p=p$ (see [2], Theorem 6 and its proof). From (*), Lemma 1, (i) and Lemma 3, we obtain

$$\frac{E}{p}=p-1,\ u=1,\ \bar{d}_p=\frac{N(p^2-2)}{p(p-1)}.$$

Now suppose that $(-A)^{p-1}\equiv 1 \pmod{p^2}$. Let $\mathfrak{a}$ denote the ideal in K generated by p and $-A-\alpha$:

$$\mathfrak{a}=(p,\ -A-\alpha).$$

Then $\mathfrak{q}\mathfrak{a}$ is divisible by every prime factor of p, $d_p=p-2$, $N(\mathfrak{a})=p^2$ and $p=\mathfrak{q}\prod\mathfrak{p}_i^{e_i}$, $N(\mathfrak{p}_i)=p^{f_i}$, $\sum f_i=2$ ([2], Theorem 6 and its proof). If $p=2$, then $d_p=0$, $E=1$, $u=0$, $\bar{d}_p=0$. If $p\neq 2$, $\mathfrak{a}$ cannot be a prime ideal or the square of a prime ideal, since $N(\mathfrak{q})=p$. Hence $\mathfrak{a}=\mathfrak{p}_1\mathfrak{p}_2$, $\mathfrak{p}_1\neq\mathfrak{p}_2$, $p=\mathfrak{q}\mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}$, $e_1>e_2$. Since $\mathfrak{q}\mathfrak{a}^{e_1}$ is divisible by p, $\dfrac{\alpha(A+\alpha)^{e_1}}{p}$ is an integer of K. Hence $e_1\geqq p-1$ ([2], Theorem 6, (2). Note that $r_p=1$). Now the result follows from Lemma 1, (g), Lemma 2, Theorem 1 and [2], Theorem 3, (1).

4. Further application of Lemma 1

In this section we study an algebraic number field K of prime degree such that every prime ideal is unramified in $\bar{K}/K$.

Theorem 4. *Let K be an algebraic number field of prime degree l, $\bar{K}$ the Galois closure of $K/\mathbb{Q}$, G the Galois group of $\bar{K}/\mathbb{Q}$, and d the discriminant of K.*

(1) *If every prime ideal is unramified in $\bar{K}/K$, G is a simple group.*

(2) *If $(l, d)=1$ and if every prime ideal in K has ramification index 1 or l with respect to $K/\mathbb{Q}$, then every prime ideal is unramified in $\bar{K}/K$.*

Proof. Suppose that every prime ideal is unramified in $\bar{K}/K$. If p is a prime factor of d, then

$$p=\mathfrak{p}^l,\quad \mathfrak{p} \text{ a prime ideal}$$

in K. Let $N\neq G$ be a normal subgroup of G, F its fixed field, and H the Galois group of $\bar{K}/K$. Let p_0 be a prime factor of the discriminant of F. Then the ramification index of p_0 with respect to $F/\mathbb{Q}$ is equal to l, since $p_0|d$. Hence $[G:N]=[F:\mathbb{Q}]$ is divisible by l. Since $[G:H]=l$ is a prime number, we have

$$HN=G \quad \text{or} \quad HN=H.$$

On the other hand, since $|G|_l = 1$, we obtain $|H|_l = |N|_l = 0$. Now

$$HN/N \cong H/H \cap N.$$

Hence $HN = H$, i.e. $N \subset H$. Since $\bar{K}$ is the Galois closure of $K/\mathbb{Q}$, we obtain $N = \{1\}$. Therefore G is a simple group.

The assertion (2) follows from Lemma 1, (g).

Theorem 5. *Let l be a prime number such that $l \equiv 1 \pmod 8$ and let $A \neq 0$ be a rational integer. Then there exists an algebraic number field K of degree l with the following properties.*

(1) *The discriminant d of K is prime to A.*
(2) *Every prime ideal is unramified in $\bar{K}/K$, where $\bar{K}$ is the Galois closure of $K/\mathbb{Q}$.*
(3) *The Galois group of $\bar{K}/\mathbb{Q}$ is a non-cyclic simple group.*

Proof. For any prime factor p of $l-1$ and any $N > 0$, the congruence

$$x^2 \equiv l^l \pmod{p^N}$$

is solvable. Hence there exist integers x_1, y_1 such that

$$x_1^2 - l^l = y_1 (l-1)^{l-1}, \quad (x_1, l) = 1.$$

Put

$$(y_1, A) = p_1^{e_1} \ldots p_m^{e_m}.$$

Then, for each i, there exists an integer t_i such that

$$t_i \not\equiv 0, \; x_1 + t_i \frac{l(l-1)^{l-1}}{4} \prod_{\substack{p \mid A, \\ p \nmid y_1}} p \not\equiv 0 \pmod{p_i}.$$

In fact, if $p_i \mid (l-1)$, we can take $t_i = 1$. If $p_i \nmid (l-1)$, such a t_i always exists since $p_i \neq 2$, $p_i \nmid l(l-1)^{l-1} \prod p$. Let t be an integer such that

$$t \equiv t_i \pmod{p_i}$$

for every i. Put

$$x_2 = x_1 + \frac{tl(l-1)^{l-1} M}{2},$$

$$y_2 = y_1 + tlM \left(x_1 + \frac{tl(l-1)^{l-1} M}{4} \right),$$

where

$$M = \prod_{\substack{p \mid A, \\ p \nmid y_1}} p.$$

Then

$$x_2^2 - l^l = (l-1)^{l-1} y_2, \; (x_2, l) = 1, \; (y_2, lA) = 1.$$

This implies that

$$\{(x, y) \in \mathbb{Z} \times \mathbb{Z},\ x^2 - l^l = (l-1)^{l-1}\, y,\ (y, lA) = 1\}$$

is an infinite set. On the other hand,

$$\{(x, r) \in \mathbb{Z} \times \mathbb{Z},\ x^2 - l^l = (l-1)^{l-1}\, r^l\}$$

is a finite set (see, for example, Mordell [3], p. 265). Hence there exist integers a, b and a prime number p such that

$$a^2 - l^l = (l-1)^{l-1}\, b,\ (b, lA) = 1,\ b_p \not\equiv 0 \pmod{l}.$$

Now $f(x) = x^l + bx + b$ is irreducible (Lemma 4). Let α be a root of $f(x) = 0$, and $K = \mathbb{Q}(\alpha)$. Then ([2], Theorem 2)

$$D = N(f'(\alpha)) = b^{l-1}\, a^2.$$

If q is a prime factor of the discriminant d of K, then $q \mid b$ ([2], Theorem 2. Note that D_q is even), and $b_q \not\equiv 0 \pmod{l}$. In fact, if $b_q = ls$, $s \in \mathbb{Z}$, then $\dfrac{\alpha}{q^s}$ is a root of

$$x^l + \left(\frac{b}{q^{(l-1)s}}\right) x + \left(\frac{b}{q^{b_q}}\right) = 0$$

and so $q \nmid d$ since $q \neq l$. Hence $b_q \not\equiv 0 \pmod{l}$ and so

$$q = \mathfrak{q}^l, \quad \mathfrak{q} \text{ a prime ideal}$$

in K (Lemma 4). It is easily seen that d is prime to lA. Finally, K is not totally real, since

$$f'(x) = lx^{l-1} + b$$

has imaginary roots. By Theorem 4, we see that K satisfies the conditions (2) and (3).

Remark. Theorem 4 implies that if K is an algebraic number field of prime degree l with discriminant

$$d = f^{l-1},$$

where f is a rational integer whose prime factors are all greater than l, then the Galois group G of $\bar{K}/\mathbb{Q}$ is a simple group, i.e. G is a cyclic group of order l (so that $\bar{K} = K$) or a non-solvable simple group. By Theorem 5 we see that the latter case may happen (cf. Reichardt and Wegner [4], Satz 5).

References

[1] *D. Hilbert*, Die Theorie der algebraischen Zahlkörper, Jber. dt. Math.-Verein. **4** (1897), 175—546 (Gesammelte Abhandlungen I, 2. Aufl.).

[2] *K. Komatsu*, Integral bases in algebraic number fields, J. reine angew. Math. **278/279** (1975), 137—144.

[3] *L. J. Mordell*, Diophantine equations, London-New York 1969.

[4] *H. Reichardt* und *U. Wegner*, Arithmetische Charakterisierung von algebraisch auflösbaren Körpern und Gleichungen von Primzahlgrad, J. reine angew. Math. **178** (1937), 1—10.

[5] *K. Uchida*, Unramified extensions of quadratic number fields. I, Tôhoku Math. Journ. **22** (1970), 138—141.

[6] *K. Uchida*, Unramified extensions of quadratic number fields. II, Tôhoku Math. Journ. **22** (1970), 220—224.

[7] *Y. Yamamoto*, On unramified Galois extensions of quadratic number fields, Osaka J. Math. **7** (1970), 57—76.

Department of Mathematics, Waseda University, Nishi-Okubo 4-170, Shinjuku-ku, Tôkyô, Japan

Eingegangen 8. März 1974